Service Mesh Big Survey



Максим Чудновский & Игорь Густомясов



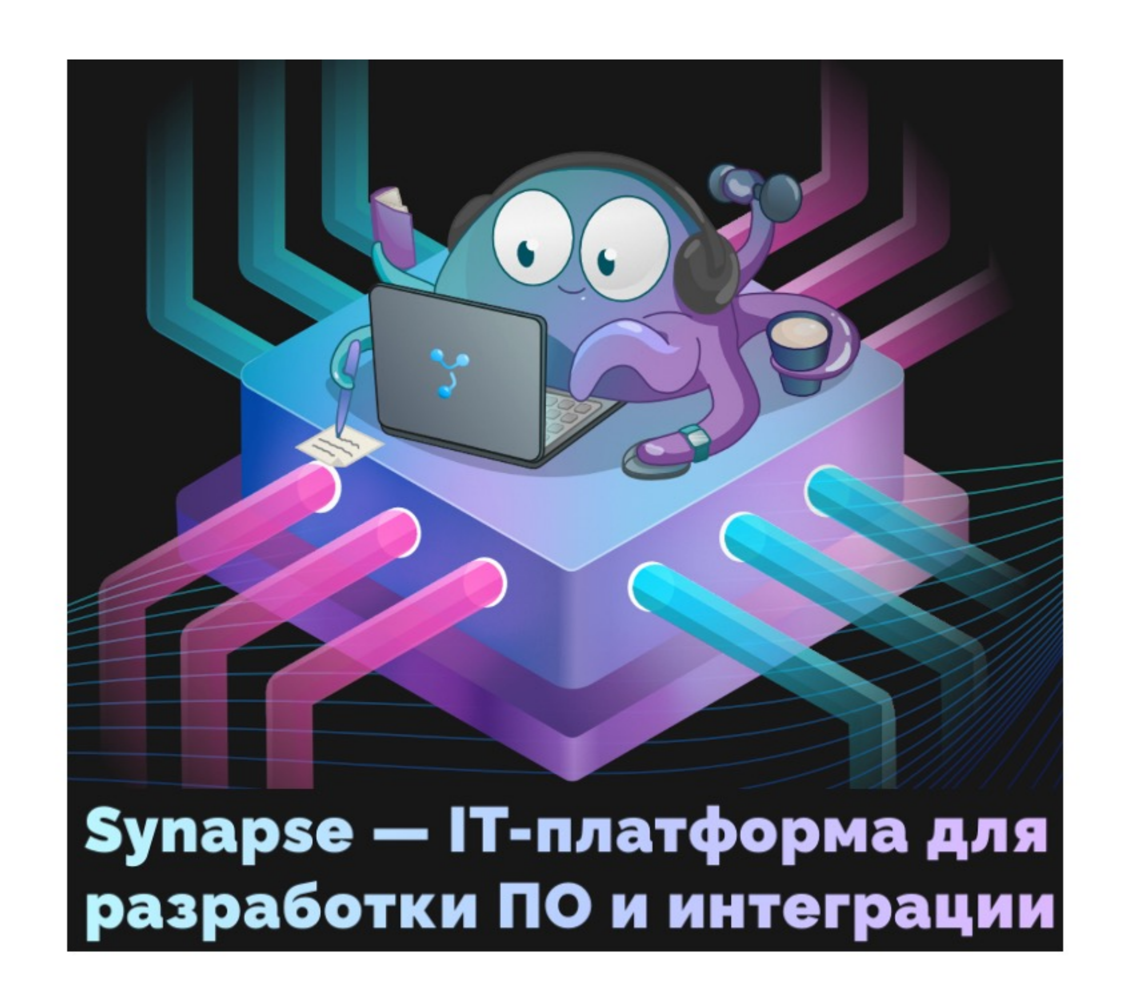
О Нас



Игорь Густомясов
Сбертех



Максим Чудновский
Сбертех





Немного теории



Что такое Service Mesh

SERVICE MESH

Control Plane

конфигурация
для Прокси

метрики

Сертификаты,
списки доступа, ...

Pod

Прокси
sidecar

Сервис

HTTP/1
HTTP/2
gRPC

Pod

Прокси
sidecar

Сервис



Control Plane

SERVICE MESH

Control Plane

конфигурация
для Прокси

метрики

Сертификаты,
списки доступа, ...

Pod

Прокси
sidecar

Сервис

HTTP/1
HTTP/2
gRPC

Pod

Прокси
sidecar

Сервис

- Назначение и распространение политик маршрутизации и балансировки трафика
- Распространение ключей, сертификатов, токенов
- Сбор телеметрии, формирование метрик мониторинга
- Интеграция с инфраструктурой безопасности и мониторинга



Data Plane

SERVICE MESH
Control Plane
конфигурация для Прокси
метрики
Сертификаты, списки доступа, ...
Pod
HTTP/1
HTTP/2
gRPC
Прокси sidecar
Прокси sidecar
Сервис
Сервис

- Маршрутизация и балансировка
- Механизмы сетевой упругости (таймауты, предохранители и т.д)
- Аутентификация и авторизация вызовов
- Отбрасывание метрик (observability)

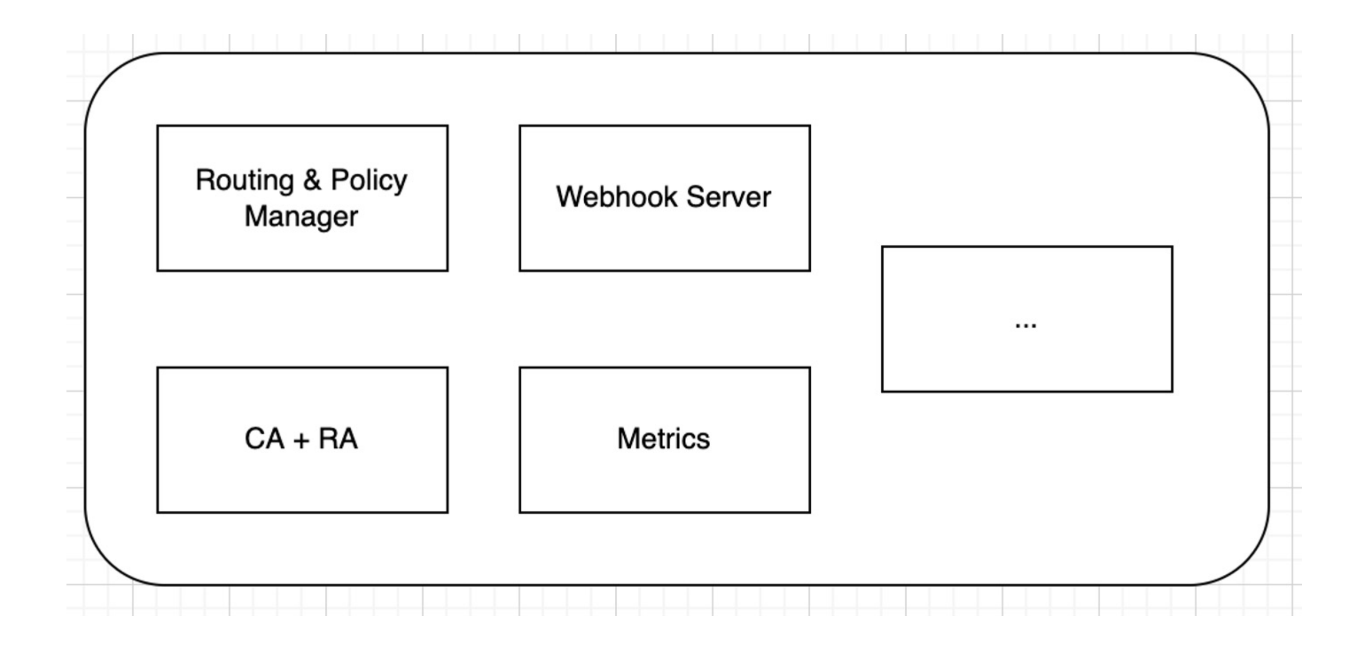


Поговорим о классификации



Control Plane. Компонентный состав

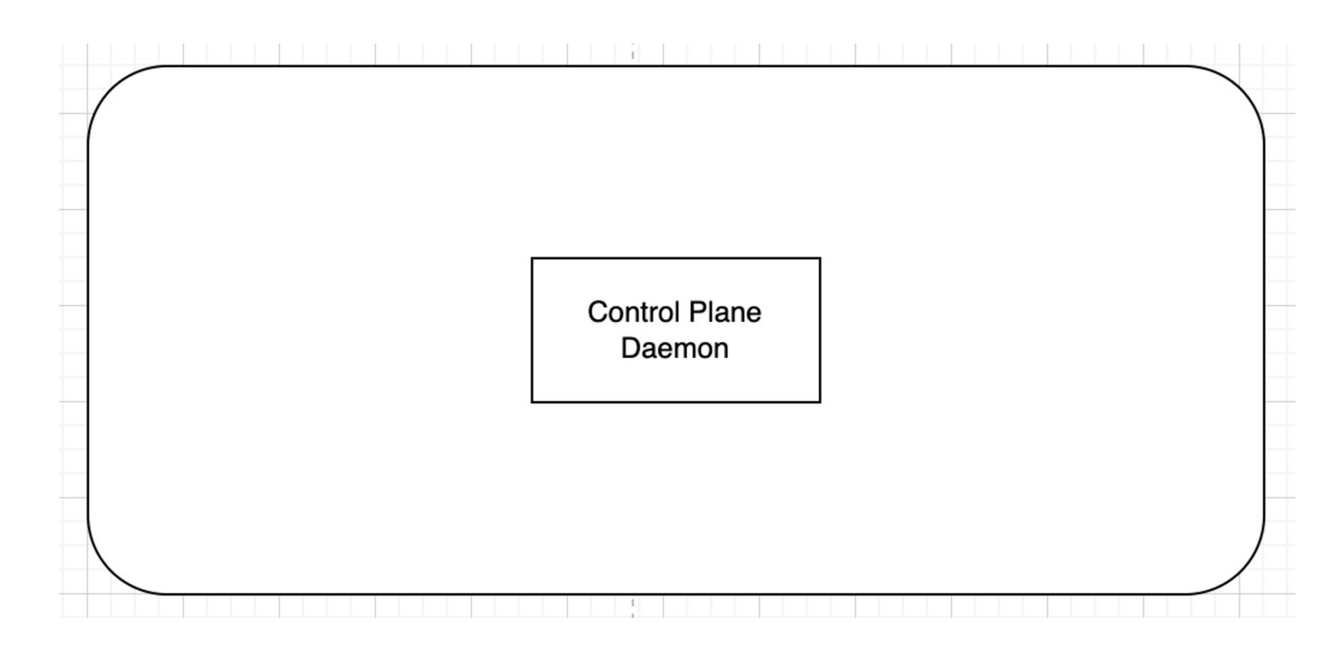
- **Микросервисы**





Control Plane. Компонентный состав

- Микросервисы
- **Монолит**





Control Plane. API

- **Пропиетарный**

```yaml
apiVersion: networking.istio.io/v1beta1
kind: VirtualService
metadata:
  name: egressgateway-kubeapi-vs
spec:
  exportTo:
    - .
  gateways:
    - mesh
  hosts:
    - kubernetes.default.svc.cluster.local
  tls:
    - match:
        - port: 443
          sniHosts:
            - kubernetes.default.svc.cluster.local
      route:
        - destination:
            host: egressgateway-kubeapi
            port:
              number: 4443
```



Control Plane. API

- Пропиетарный
- **Gateway API**

```yaml
apiVersion: gateway.networking.k8s.io/v1alpha2
kind: HTTPRoute
metadata:
  name: http
  namespace: default
spec:
  parentRefs:
  - name: gateway
    namespace: istio-ingress
  hostnames: ["httpbin.example.com"]
  rules:
  - matches:
    - path:
        type: PathPrefix
        value: /get
    backendRefs:
    - name: httpbin
      port: 8000
```



Control Plane. API

- Пропиетарный
- Gateway API
- **SMI-Spec**

```yaml
apiVersion: split.smi-spec.io/v1alpha2
kind: TrafficSplit
metadata:
  name: backend-split
  namespace: trafficsplit-sample
spec:
  service: backend-svc
  backends:
  - service: backend-svc
    weight: 500
  - service: failing-svc
    weight: 500
```



Data Plane. Компонентный состав

- **Sidecars**

sidecar
APP
pod
node

sidecar
APP
pod
node



Data Plane. Компонентный состав

- Sidecars
- **Node Daemon**

daemon
daemon
APP
pod
node
APP
pod
node



Data Plane. Компонентный состав

- Sidecars
- Node Daemon
- **Proxyless**

lib
APP
pod
node
lib
APP
pod
node



Data Plane. API

- **xDS**

VIP1
VIP2
VIP3
Route
Route
Cluster
Cluster
endpoint
endpoint
Locality 1
endpoint
Locality 2
endpoint
Locality 3



Data Plane. API

- xDS
- **Пропиетарный**

```
cat << EOF > config.json

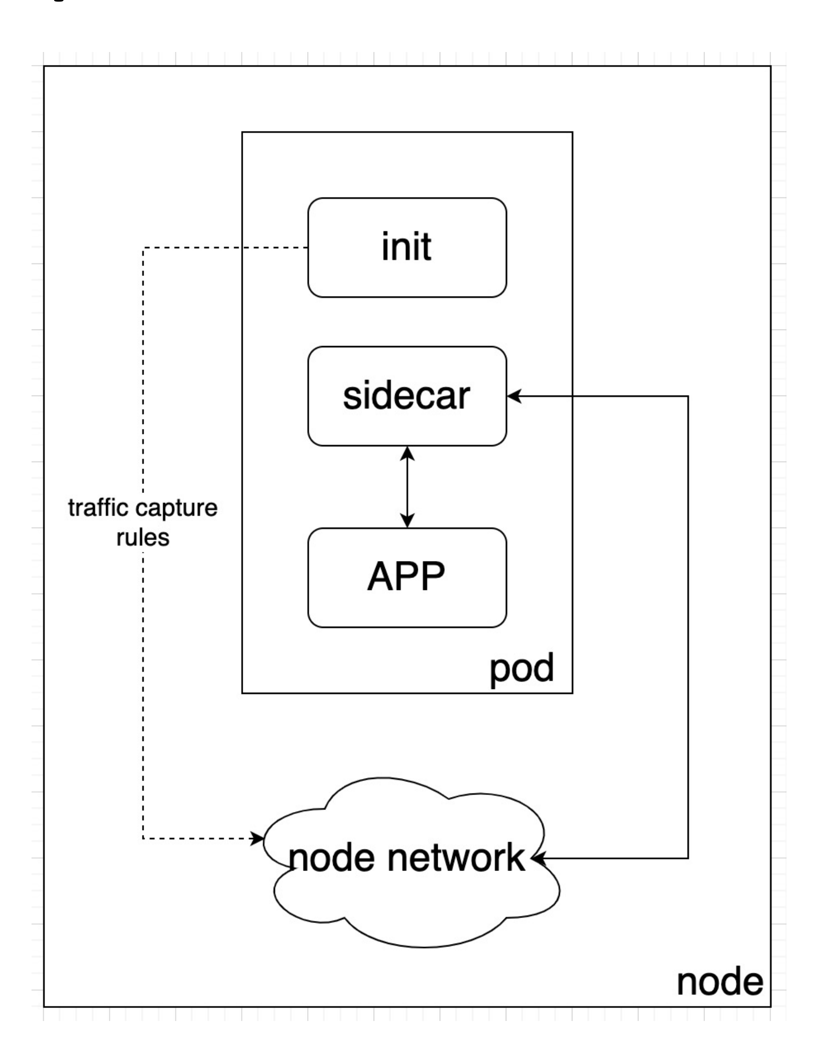
    {
        "type": "php",
        "root": "/www/blogs/scripts"
    }
EOF

sudo curl -X PUT --data-binary @config.json --unix-socket \
       /path/to/control.unit.sock http://localhost/config/applications/blogs
```



Data Plane. Traffic Capture

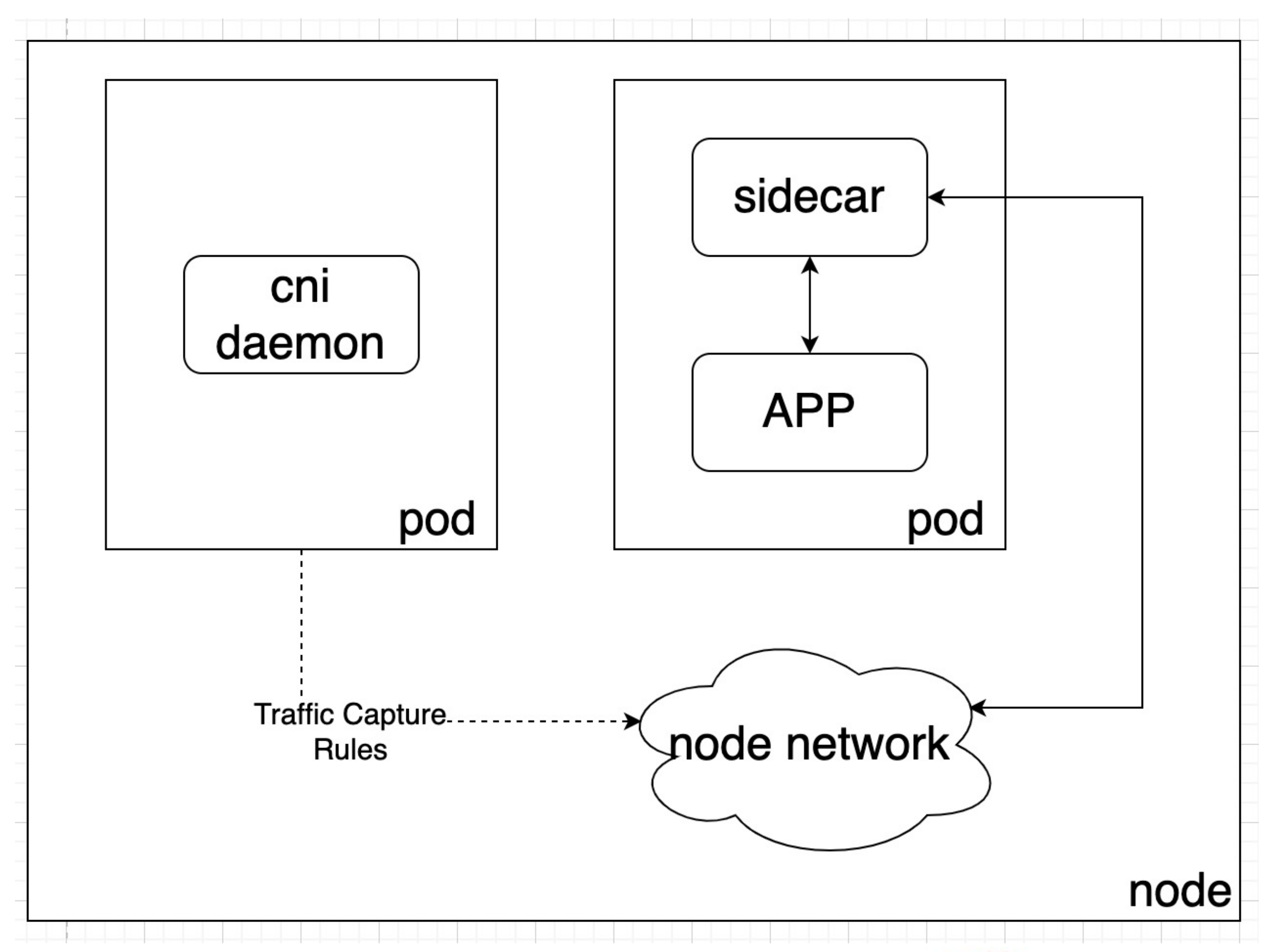
- **Pod Level**





Data Plane. Traffic Capture

- Pod Level
- **Node Level**





Из чего можно выбрать?



Istio (1/9)

Istio Mesh
Data plane
Service A
Service B
Proxy
Mesh traffic
Proxy
Ingress traffic
Egress traffic
Discovery
Configuration
Certificates
Control plane
istiod
Pilot
Citadel
Galley

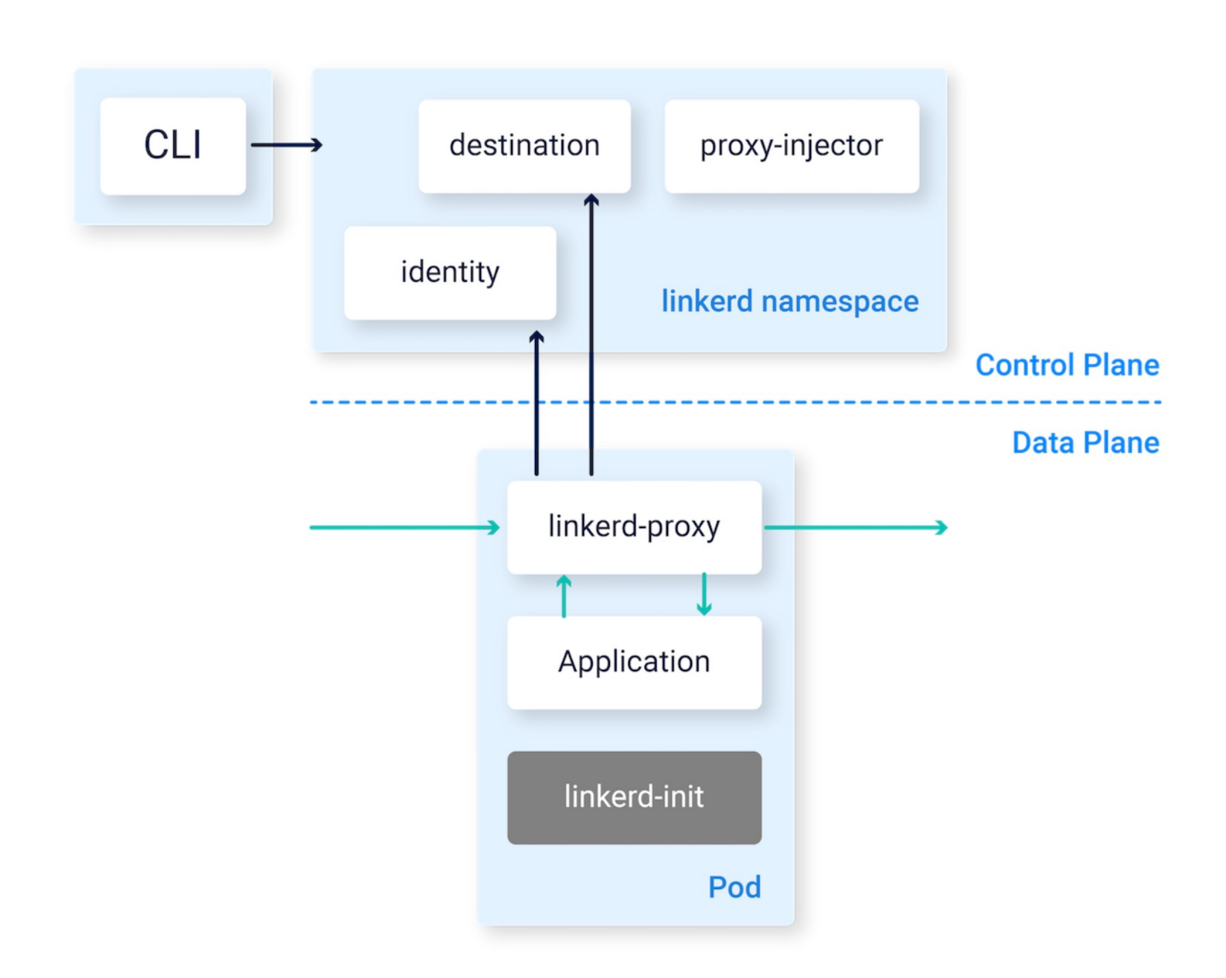
Istio Architecture

Control Plane Type	Monolith
Control Plane API	Proprietary, Gateway API, SMI*
Data Plane Type	Sidecar, Proxyless, CNI*
Data Plane API	xDS
Traffic Capture Type	Pod & Node Levels
Extensions	WASM

https://istio.io/latest/docs/ops/deployment/architecture/



Linkerd (2/9)

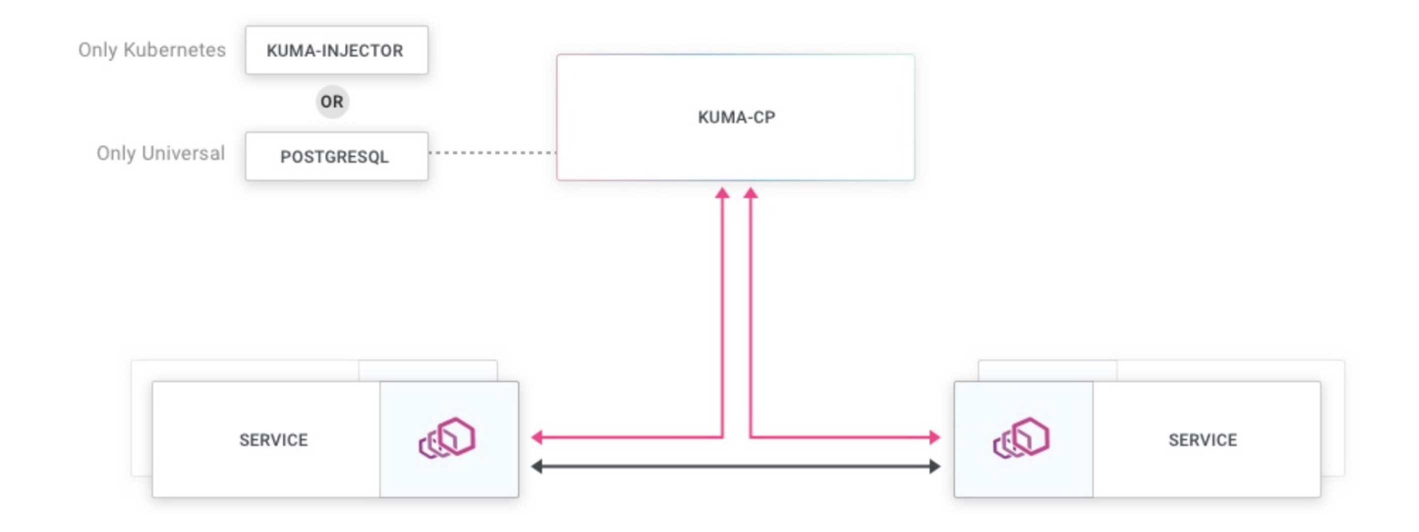


Control Plane Type	Microservices
Control Plane API	Proprietary, SMI
Data Plane Type	Sidecar
Data Plane API	Proprietary
Traffic Capture Type	Pod & Node Levels
Extensions	N/A

https://linkerd.io/2.12/reference/architecture/



Kuma (3/9)



Control Plane Type	Monolith
Control Plane API	Proprietary Gateway API
Data Plane Type	Sidecar
Data Plane API	xDS
Traffic Capture Type	Pod & Node Level
Extensions	N/A

https://kuma.io/docs/1.8.x/explore/overview/#components



Nginx (4/9)

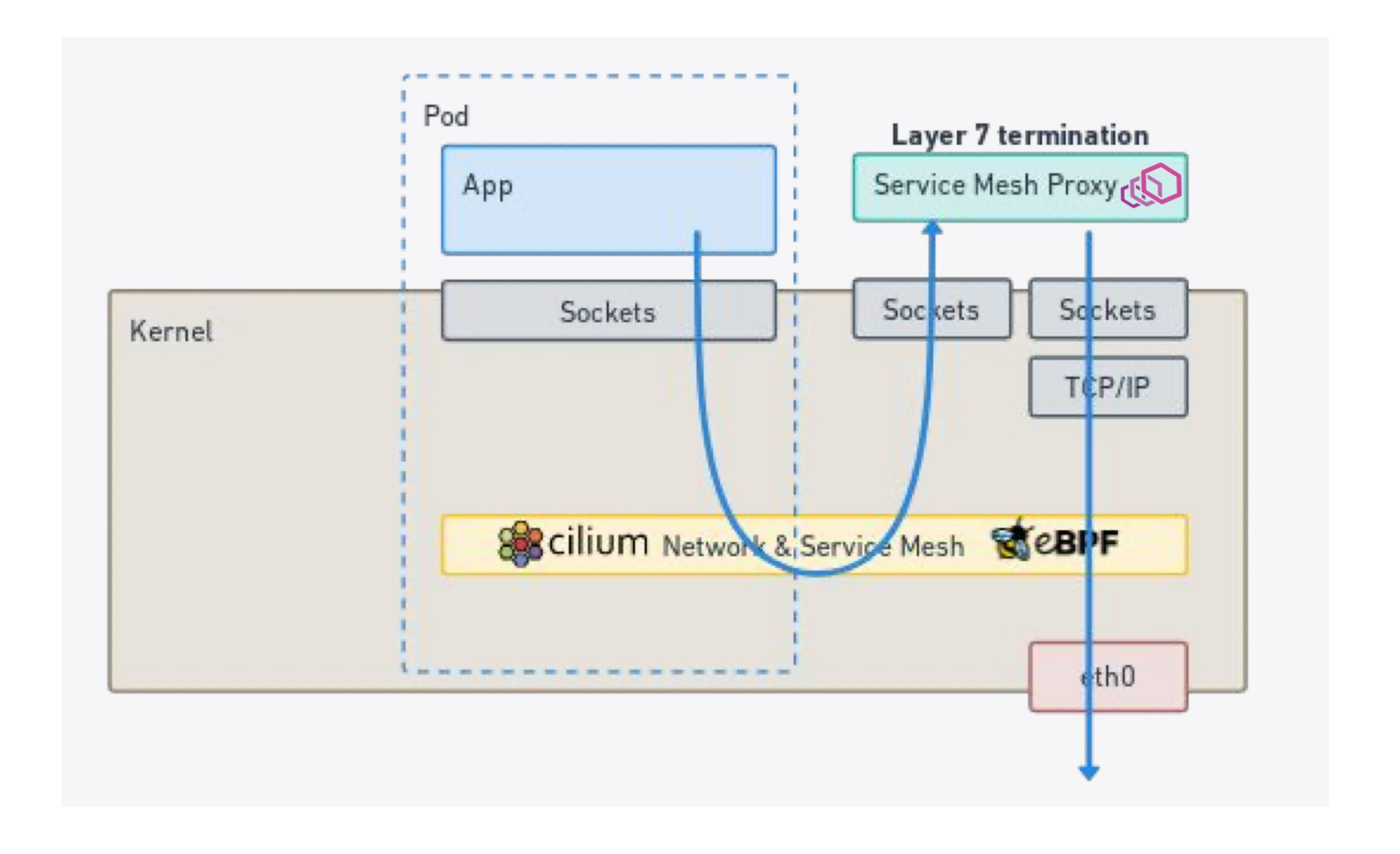
Observability Plane
Grafana
OpenTelemetry
Prometheus
NGINX Service Mesh CLI
Control Plane
Kubernetes API Server
Service Config
Application Config
Spire Server
Identity
NGINX Service Mesh Controllers
Topology
Endpoints
Policies
Metrics Server
NATS Message Bus
Spire Agent
Data Plane
NGINX Ingress
NGINX Egress
Pod
App Workload
Agent

Control Plane Type	Microservices
Control Plane API	SMI
Data Plane Type	Sidecar
Data Plane API	Proprietary
Traffic Capture Type	Pod Level
Extensions	N/A

https://docs.nginx.com/nginx-service-mesh/about/architecture



Cilium Service Mesh (5/9)

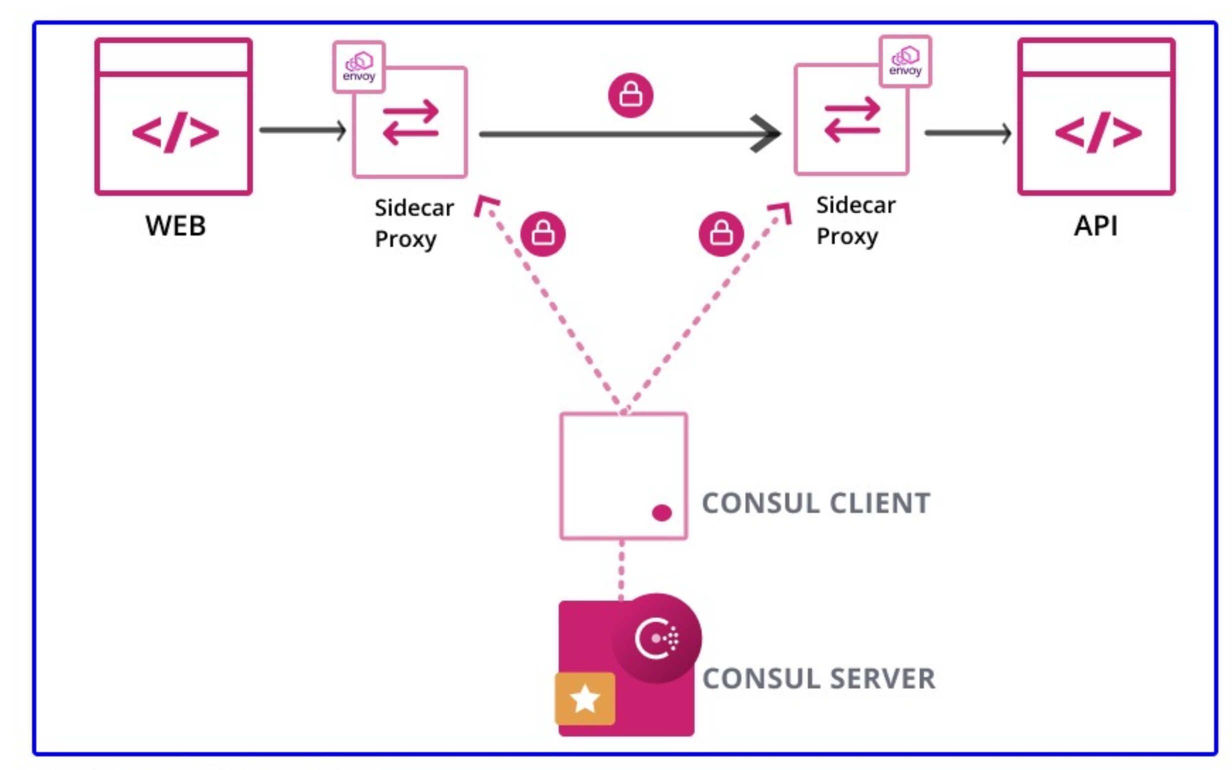


Control Plane Type	Microservices
Control Plane API	Propietary
Data Plane Type	CNI + Node Daemon
Data Plane API	XDS
Traffic Capture Type	Node Level (eBPF)
Extensions	WASM



https://docs.cilium.io/en/stable/gettingstarted/#service-mesh

Consul (6/9)

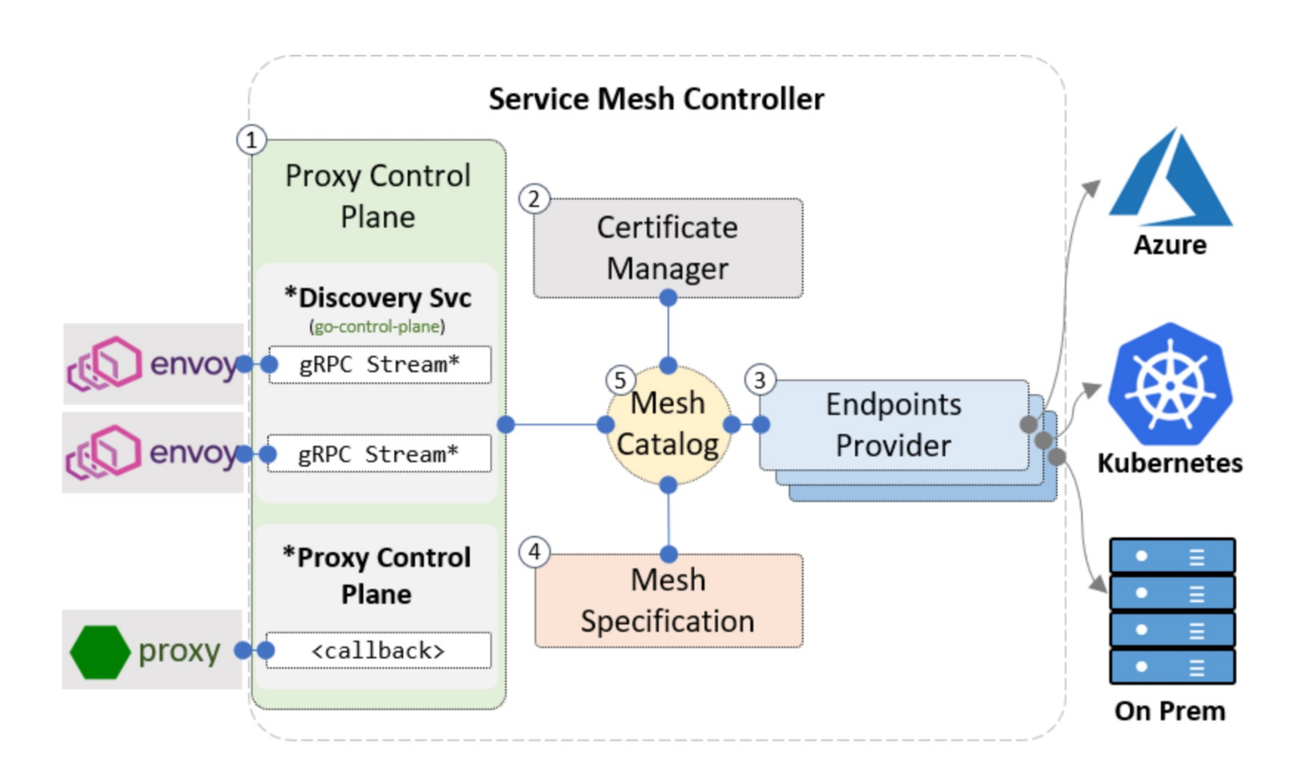


Control Plane Type	Microservices
Control Plane API	Propietary, SMI
Data Plane Type	Sidecar
Data Plane API	XDS
Traffic Capture Type	Pod Level
Extensions	N/A

https://learn.hashicorp.com/tutorials/consul/service-mesh-application-secure-networking?in=consul/kubernetes



Open Service Mesh (7/9)

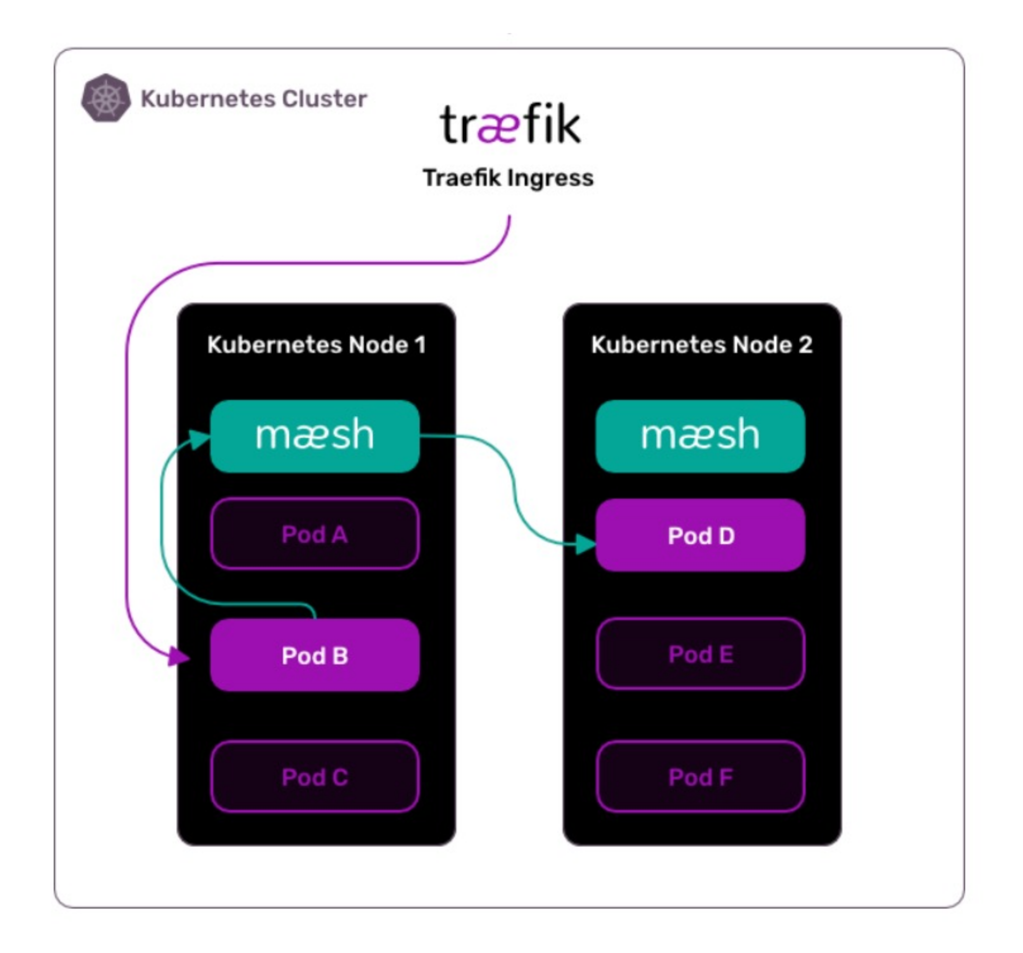


Control Plane Type	Microservices
Control Plane API	SMI
Data Plane Type	Sidecar
Data Plane API	XDS
Traffic Capture Type	Pod Level
Extensions	N/A

https://release-v1-2.docs.openservicemesh.io/docs/overview/osm_components/



Traefic (8/9)

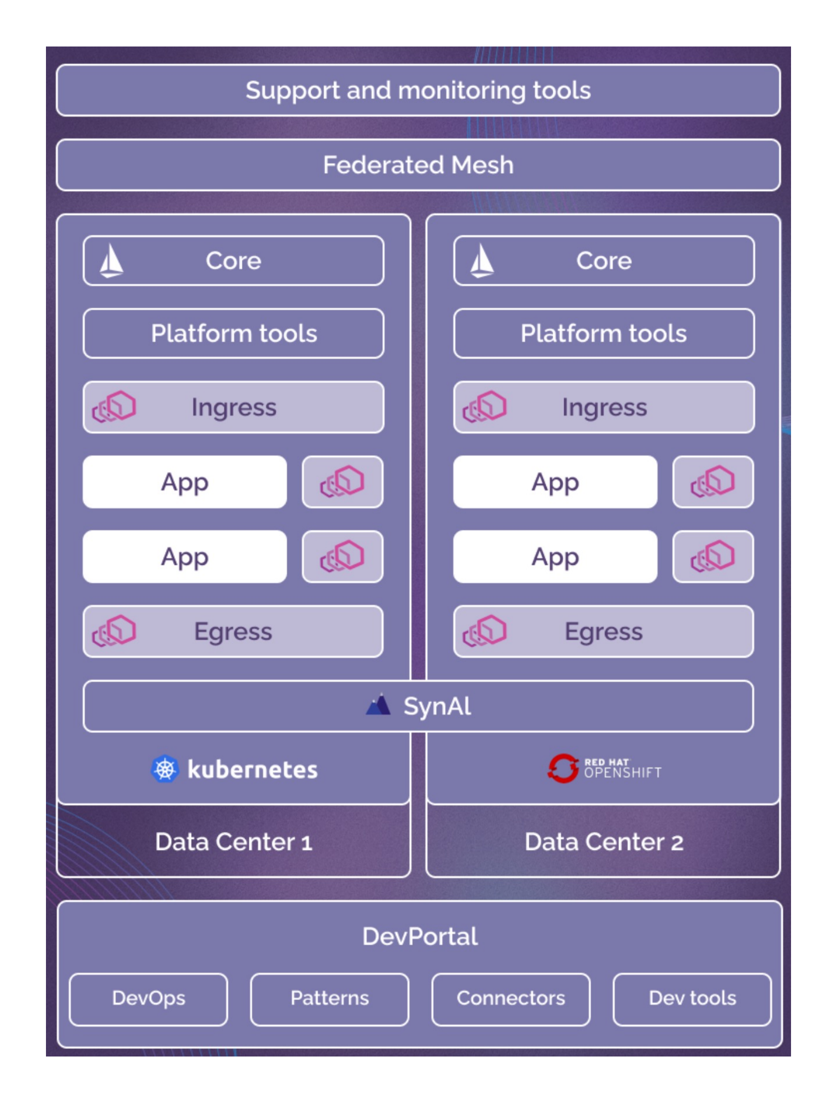


Control Plane Type	Microservices
Control Plane API	SMI
Data Plane Type	Node Daemon
Data Plane API	XDS
Traffic Capture Type	Nod Level
Extensions	N/A

https://doc.traefik.io/traefik-mesh/



Synapse Service Mesh (9/9) – **сделано спикерами**



http://getsynapse.io/products/service-mesh

Control Plane Type	Microservices
Control Plane API	Propietary, Gateway API, SMI*
Data Plane Type	Sidecar, Proxyless*, CNI*
Data Plane API	XDS, LazyXDS
Traffic Capture Type	Pod & Node Levels (inc. eBPF)
Extensions	WASM



Мы всех посмотрели, но как выбирать?



Наш опыт

- **Platform V Synapse Service Mesh**



Наш опыт

- Platform V Synapse Service Mesh
- **Первые инсталляции в 2018 году**



Наш опыт

- Platform V Synapse Service Mesh
- Первые инсталляции в 2018 году
- **На сегодня**
  - **200+ инсталляций в промышленной среде**
  - **17 команд сопровождения**



Масштабирование

- **Количество кластеров (федерация vs межкластерный меш)**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Масштабирование

- **Количество кластеров (федерация vs межкластерный меш)**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Масштабирование

- Количество кластеров (федерация vs межкластерный меш)
- **Размеры кластеров (стоимость vs надежность)**
  - ***Ноды***
  - ***Рабочие нагрузки***
  - ***Поды***
  - ***Сервисы***

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Масштабирование

- Количество кластеров (федерация vs межкластерный меш)
- **Размеры кластеров (стоимость vs надежность)**
  - ***Ноды***
  - ***Рабочие нагрузки***
  - ***Поды***
  - ***Сервисы***

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Взаимное влияние

- **Blast Radius**
  - **в случае компрометации секретов или пода в целом**
  - **в случае, когда у соседа что-то пошло не так**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Взаимное влияние

- **Blast Radius**
  - **в случае компрометации секретов или пода в целом**
  - **в случае, когда у соседа что-то пошло не так**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Сложности эксплуатации

- **Сложность конфигурирования (простота vs гибкость)**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Сложности эксплуатации

- **Сложность конфигурирования (простота vs гибкость)**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Сложности эксплуатации

- Сложность конфигурирования (простота vs гибкость)
- **Сила сообщества**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Сложности эксплуатации

- Сложность конфигурирования (простота vs гибкость)
- **Сила сообщества**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Сложности эксплуатации

- Сложность конфигурирования (простота vs гибкость)
- Сила сообщества
- **Поддержка открытых стандартов**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Сложности эксплуатации

- Сложность конфигурирования (простота vs гибкость)
- Сила сообщества
- **Поддержка открытых стандартов**

Control Plane Type
Control Plane API
Data Plane Type
Data Plane API
Traffic Capture Type
Extensions



Подведем итоги



Итоги

- **Теперь мы знаем все о том, каким бывает Service Mesh в теории**



Итоги

- Теперь мы знаем все о том, каким бывает Service Mesh в теории
- **Мы понимаем, какие решения доступны на практике**



Итоги

- Теперь мы знаем все о том, каким бывает Service Mesh в теории
- Мы понимаем, какие решения доступны на практике
- **Мы знаем, с чем можем столкнуться в продакшене**



Итоги

- Теперь мы знаем все о том, каким бывает Service Mesh в теории
- Мы понимаем, какие решения доступны на практике
- Мы значем, с чем можем столкнуться в продакшене
- **Золотого топора как не было, так и нет**



Написать нам

- IVGustomyasov.SBT@sberbank.ru
- MMChudnovskiy@sberbank.ru





Оценить доклад

